CYBELLUM

Product Security Dive:

EU Cyber Resilience Act

Overview

The Cyber Resilience Act (CRA) is a cyber-security regulation for the EU proposed on 15 September 2022 by the European Commission for improving cybersecurity and cyber resilience in the EU through common cybersecurity standards for products with digital elements in the EU.

The act will come into force and begin implementation in 2024 and is expected to be completed over a 36-month period, making it yet unclear what enforcement will look like for organizations. It is important to mention that these timelines are often dynamic and must be reviewed as time progresses.

In response to market needs, the Cybellum Product Security Platform, a leading product cybersecurity assessment and management platform, provides comprehensive support for the CRA requirements. This document reviews its capabilities against these requirements.

To review the Cyber Resilience Act, see the proposal text on the EU's website.

The latest news on EU cybersecurity policies can be found at Timeline- cybersecurity.

Analysis

Scope

The CRA applies to products that have connectivity to a network or a device. While it is a general regulation, there are stated exceptions to product categories that are covered under other regulations (Article 2, Scope, 2-4):

Product Type	Applicable Existing Regulation	Details
Medical devices	(EU) 2017/745	Clinical investigation and sale of medical devices for human use
In vitro diagnostic (IVD)	(EU) 2017/746	In vitro diagnostic medical devices
Motor vehicles	(EU) 2019/2144	Type-approval requirements for motor vehicles and their trailers
Civil aviation	(EU) 2018/1139	Establishment of a European Aviation Agency to unify standards, including cybersecurity

Note: Devices or vehicles may still be covered in cases that involve an end-user interface that collects information.

In addition, the following products are also out-of-scope:
Products developed for national security or military purposes or to products specifically designed to process classified information (Article 2, Scope, 5).

Requirements

The CRA lists requirements in three main categories:

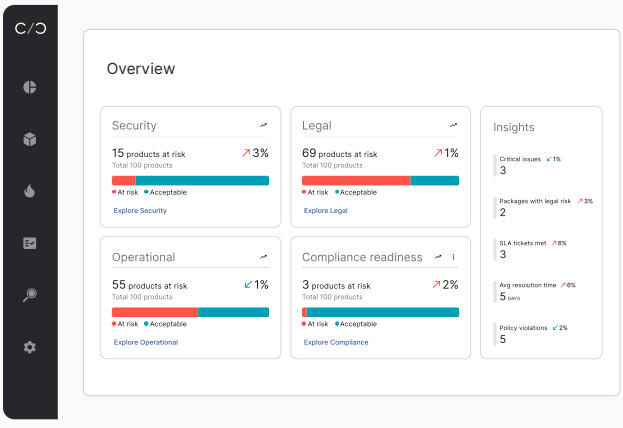
1. **Essential security requirements -** According to Article 5, products in scope of CRA must meet the essential requirements set out in Section 1 of Annex I.
2. **Security processes -** According to Article 5, the processes put in place by the manufacturer must comply with the essential requirements set out in Section 2 of Annex I.
3. **Reporting Requirement -** According to Article 11, the manufacturer must report to ENISA any actively exploited vulnerability contained in its products within 24 hours of becoming aware of it.

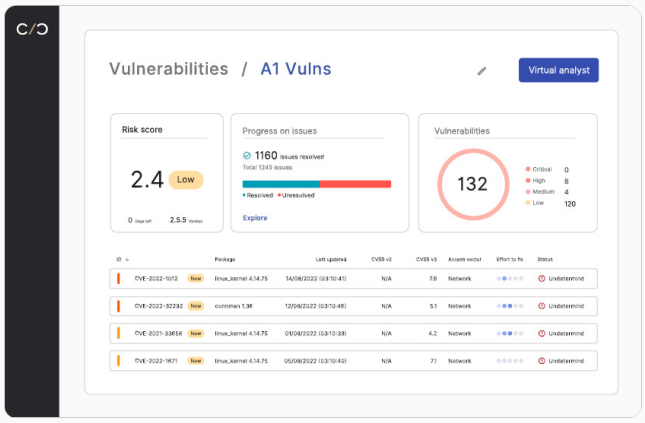
The following section provides a detailed review of these requirements and how the Product Security Platform solution supports them. The following section provides a detailed review of these requirements and how the Product Security Platform solution supports them.

Essential Cybersecurity Requirements

Annex I lists the essential cybersecurity requirements for the products in the scope of the CRA:

1. **Security Requirements Relating To The Properties Of Products With Digital Elements**

Item	Requirement	How Cybellum Addresses Each Requirement
1 (1)	Products must provide an appropriate level of cybersecurity based on the risks	Cybellums' Product Security Platform provides both engineering level and governance level capabilities to ensure full product security is reached: • During design and development: ◦ Ability to assess the security during the design stage using virtual SBOMs ◦ Create and manage SBOM, and HBOM at the product and component levels ◦ Identify and track vulnerabilities across product versions ◦ Analyze OS security hardening configurations against defined policies • During production / operational use: ◦ Incident response capabilities allow for continuous monitoring of new vulnerabilities, along with investigation and treatment capabilities for any detected threats that actually impact products 

Item	Requirement	How Cybellum Addresses Each Requirement
1 (2)	Products must be delivered without any known exploitable vulnerabilities	Cybellum's Product Security Platform provides a comprehensive suite of capabilities around Vulnerability Management which allows for policy-based enforcement of vulnerability mitigations. The manufacturer can track vulnerabilities, including coding weaknesses, throughout the full product lifecycle, ensuring secure use at all stages. 
1 (3) (a)	Default configuration must be secure	The Product Security Platform's OS hardening capabilities are designed for: • Incorporated FOSS and 3rd party components, verify security hardening applied correctly at runtime vs running in an overly privileged context. • Identify security-sensitive default settings around encryption, authentication, logging, interfaces, etc. • Confirm hardened values are set by default by security standards vs convenience. • Enumerate any default accounts, passwords, and SSH keys included in the system and verify these have been changed from common defaults and follow security best practices in terms of password strength and SSH key encryption.
1 (3) (b)	Ensure protection from unauthorized access	Through OS Hardening, the product security platform can help: • Identify authentication mechanisms enforced across all external interfaces, including service APIs, management interfaces, and consoles. • Check authentication scheme is robust and standardized like OAuth2, and SAML, not custom auth. • Validate certificate/key-based authentication parameters including encryption strength.

Item	Requirement	How Cybellum Addresses Each Requirement
1 (3) (c)	Protect the confidentiality of stored, transmitted, or otherwise processed data (with encryption, etc.)	The Product Security Platform can automatically identify confidentiality breaches using its requirements validation technology. Product security teams can: • Identify hard-coded credentials Flag potential personal data that falls outside a given policy • Detect cryptography-related characteristics (e.g. encryption algorithm, encryption key length) • Identify the existence of specific confidentiality mechanisms
1 (3) (d)	Protect the integrity of data/applications	Through OS Hardening, the product security platform can help to protect against data integrity risks.
1 (3) (f)	Resilience of services against mitigation of denial of service attacks	Through its vulnerability management and OS hardening capabilities, the Product Security Platform enhances the resilience of services.
1 (3) (g)	Minimize the negative impact on the availability of other devices/services Minimize the negative impact on the availability of other devices/ services	The Product Security Platform enables device security throughout the full product lifecycle, reducing cyber risk and managing it continuously. thus minimizing the potential impact on other devices.
1 (3) (h)	Limit attack surfaces, including external interfaces	Limiting attack surfaces and external interfaces includes OS Hardening and Exploit Mitigations activities to: • Identify and remove unused code, including debug interfaces, as it unnecessarily expands the attack surface. • Harden binaries by identification of Exploit Mitigation mechanisms against attacks like return-oriented programming (ROP) which rely on control flow hijacking.
1 (3) (i)	Use appropriate exploitation mitigation	Cybellum's Product Security Platform limits the attack surface through vulnerability management, validating adherence to OS hardening, and other security requirements, including post-production incident response. Some examples include: • Detecting and managing OS Hardening violations. • Detecting defensive compiler mitigations capabilities. • Detection of exploitation systems/libraries (whether open source or commercial) as unsafe software that should be removed from released products.
1 (3) (j)	Record activity including access to or modification of data, services or functions	Cybellum's Product Security Platform can identify logging and auditing libraries.

Item	Requirement	How Cybellum Addresses Each Requirement
1 (3) (k)	Address vulnerabilities through updates and notifications to users	**Update Mechanism** • Cybellum's Product Security Platform can help identify the presence of an automatic update mechanism for delivering security patches to users. **Vulnerability Monitoring** • Cybellum's Product Security Platform provides a facility for continuous vulnerability monitoring via interfaces to threat intelligence feeds like CVE and NVD to power notifications. • The SBOM provided by the platform is used to detect vulnerable library components.

Security Processes

Annex I lists the specific requirements for the processes the manufacturer must maintain:

2. Vulnerability Handling Requirements

Item	Requirement	How Cybellum Addresses Each Requirement
2 (1)	Create SBOM and vulnerability list	The Product Security Platform automates various product security functions, to support SBOMs and vulnerability lists via workflow automations to update SBOMs and generate VEX reports to give greater context to a device's risk.
2 (2)	Address and remediate vulnerabilities without delay	The Product Security Platform offers a streamlined approach to vulnerability management, enabling organizations to quickly identify, prioritize, and remediate vulnerabilities across their software portfolio. It provides automated discovery, real-time tracking, integrated workflow management, actionable guidance, and automated patch validation, empowering organizations to maintain a secure software supply chain.
2 (3)	Regularly test the security of the product	Cybellum's platform provides tracking the treatment of vulnerabilities across software builds and continuous monitoring of vulnerabilities.
2 (4)	Publicly disclose information about fixed vulnerabilities	The Product Security Platform provides: **Vulnerability Database** A maintained database of vulnerabilities identified across the product portfolio. Disclosure reports can leverage this data. **Remediation Tracking** The system tracks the remediation of vulnerabilities through the development processes. Reports can show the lifecycle from discovery to remediation.

Item	Requirement	How Cybellum Addresses Each Requirement
2 (4)	Publicly disclose information about fixed vulnerabilities	**Dashboards and Reporting** Product security dashboards and reports include disclosure-friendly information on addressed vulnerabilities like timeline, severity, effects, and remediation details. **CVE Mapping** Vulnerabilities can be mapped to CVE IDs where applicable to simplify public disclosure with standard references. Furthermore, the platform can generate VEX reports that can be shared with 3rd parties, testifying if vulnerabilities are or aren't impacting a product.
2 (5)	Enforce a policy on coordinated vulnerability disclosure	The Product Security Platform allows companies to implement a structured, more automated vulnerability disclosure. **Automated Workflows** Automated workflows can enforce the phases of CVD • Initial identification of a vulnerability, discovery of its impact on the company's product, and the collection of evidence necessary for disclosure.
2 (6)	Facilitate sharing of vulnerability information from users into the company	Cybellum facilitates the sharing of vulnerability information from external users into the company through: **Triage and Validation** Automated workflows can intake reports from users and initiate analysis by product security teams to reproduce and validate reported bugs. **Centralized Tracking** Store and track all vulnerability reports from users in the same system used internally, for end-to-end management.
2 (7)	Provide secure software updates	Secure software updates are supported in the Product Security Platform by analyzing, scanning, and triaging risks discovered within new software versions as they become available. This allows for product security teams to validate SBOMs and management vulnerabilities with fewer resources.
2 (8)	Release security updates without delay and free of charge	The Cybellum Product Security Platform accelerates the pace at which software updates are assessed. When introduced as part of a CI/CD build pipeline, software updates are processed automatically by the platform. This provides the product security team with an efficient method to assess, escalate, and track the progress of security updates. This eventually leads to a faster release process overall.

Reporting Requirement

The manufacturer is expected to report vulnerabilities to ENISA. There are no specific requirements as to the format or tool to use, as this may differ between EU Member States.

The Cybellum Product Security Platform provides flexible reporting formats for vulnerability information exchange:

- VEX
- XLS
- REST API

About us

CYBELLUM IS WHERE TEAMS DO PRODUCT SECURITY.

Device manufacturers such as Jaguar Land Rover, Supermicro, Danaher, and Faurecia use Cybellum's Product Security Platform and services to manage cybersecurity risk and compliance across business units and lifecycle stages. From SBOM to Vulnerability Management, Compliance Validation, and Incident Response, teams ensure their connected products are fundamentally secure and compliant – and stay that way.

Learn more about Product Security

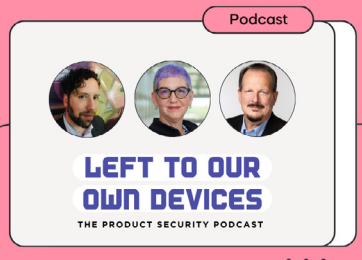
Blogs

Introduction to Medical Device Security Standards and Regulations

Rolling Regulations: Embrace Them, Don't Chase Them

Keeping the Software Supply Chain Accountable with SBOMs

Podcasts



Knowledge Base

Breaking down the FDA's 2023 Premarket Cybersecurity Requirements

Learn More →

Mastering TARA and Risk Management with itemis and Cybellum

Learn More →

SBOM for Connected Devices: Getting it Right

Learn More →

More about the Product Security Platform